IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Ferri et al.**	§	Group Art Unit: **2134**
	§	
Serial No. **10/718,064**	§	Examiner: **Tran, Ellen C.**
	§	
Filed: **November 20, 2003**	§	Customer No.: **50170**
	§	
For: **Method of Authenticating**	§	
Digitally Encoded Products	§	
Without Private Key Sharing		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPELLANTS' BRIEF (37 C.F.R. § 41.37)

This Appeal Brief is in furtherance of the Notice of Appeal filed December 9, 2008 (37 C.F.R. § 41.31).

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying Fee Transmittal.

I.   Real Party in Interest

The real party in interest in this appeal is the following party: International Business Machines Corporation.

II.   Related Cases

With respect to other appeals and interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

III.   Jurisdiction

The Board has jurisdiction under 35 U.S.C. § 134(a). The Examiner mailed a final rejection on September 9, 2008, setting a three-month shortened statutory period for response. The time for responding to the final rejection expired on December 9, 2008. Rule 134. A notice of appeal was filed on December 9, 2008. The time for filing an appeal brief is two months after the filing of a notice of appeal. Bd.R. 41.37(c). The time for filing an appeal brief expired on February 9, 2009. The appeal brief is being filed on February 9, 2009.

IV. Table of Contents

V. Table of Authorities

In re Bond, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990)....8

In re Lowry, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994)
....8

Kalman v. Kimberly-Clark Corp., 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir.
1983) 8

In re Fritch, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992)..............15

VI.   **Status of Amendments**

No amendment was filed after final rejection.

VII.   **Grounds of Rejection to be Reviewed on Appeal**

The grounds of rejection to be reviewed on appeal are:

● The rejection of claims 1-3 under 35 U.S.C. § 102(e) as being allegedly anticipated by Bhagavatula et al. (U.S. Patent No. 7,140,036); and

● The rejection of claims 4-8 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Bhagavatula et al. (U.S. Patent No. 7,140,036) in view of Graves et al. (U.S. Publication No. 2004/0177047).

VIII. Statement of Facts

1.   In rejecting claims 1-3, the Examiner cites Bhagavatula as teaching the features recited in claims 1-3.

2.   In rejecting claims 4-8, the Examiner cites Bhagavatula and Graves as teaching the features recited in claims 4-8.

3.   In rejecting claim 1, the Examiner cites Bhagavatula column 8, lines 20-25 as teaching a client system transmitting a request of authentication of the product to a server system.

4.   In rejecting claim 1, the Examiner cites Bhagavatula column 7, line 57, to column 8, line 25 as teaching certifying that the product originates from the entity using sensitive information of the entity stored on the server system.

5.   In rejecting claim 1, the Examiner cites Bhagavatula column 8, lines 54-67 as teaching returning a representation of the certification to the client system.

6.   In rejecting claim 4, the Examiner acknowledges that Bhagavatula does not teach automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key.

7.   In rejecting claim 4, the Examiner cites Graves paragraphs [0050], [0052], and [0053] as teaching automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key.

8.   In rejecting claim 7, the Examiner cites Graves paragraphs [0050], [0052], and [0053] as teaching the client system invoking a remote command on the server system, the server system verifying whether the remote command is included in a predefined list stored on the server system, the list including at least one remote command for satisfying the request of authentication, and the server system executing the remote command if included in the list.

9.   In rejecting claim 8, the Examiner cites Bhagavatula column 8, lines 20-31 as teaching a client system transmitting a request of authentication of the product to a server system.

10.   In rejecting claim 8, the Examiner cites Graves paragraphs [0050], [0052], and [0053] as teaching generating a digital signature of the product using a private key of the entity stored on the server system.

11.   In rejecting claim 8, the Examiner cites Graves paragraph [0056] as teaching returning the digital signature to the client system, wherein the digital signature certifies that the product originates from the entity.

IX. Argument

A. Rejection under 35 U.S.C. § 102(e), Claims 1-3

The Final Office Action rejects claims 1-3 under 35 U.S.C. § 102(e) as being allegedly anticipated by Bhagavatula et al. (U.S. Patent No. 7,140,036). This rejection is respectfully traversed.

1. Claims 1-3

Claim 1 reads as follows:

1. A method of authenticating a digitally encoded **product being originated by an entity** having at least one authorized subject, the method including the steps of:

a client system transmitting a request of authentication of the product to a server system,

the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:

certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and

returning a representation of the certification to the client system. (emphasis added)

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Appellants respectfully submit that Bhagavatula does not identically show every element of claim 1 arranged as they are in the claim. Specifically, Bhagavatula does not teach the elements emphasized above in claim 1.

Bhagavatula is directed to centralized identity authentication for use in connection with a communications network. Bhagavatula registers users of the communications network such that each registered user's identity is uniquely defined and determinable. Bhagavatula also registers a plurality of vendors having a presence on the communications network. The registered vendors selectively transact with registered users, wherein the transactions include: (i) the registered vendor selling goods and/or services to the registered user; (ii) the registered vendor granting the registered user access to personal records

maintained by the registered vendor; and/or (iii) the registered vendor communicating to the registered user personal information maintained by the registered vendor. The method also includes each user's identity being authenticated over the communications network prior to completion of transactions between registered vendors and registered users.

Thus, Bhagavatula merely authenticates users and vendors that access the communications network. The Final Office Action alleges that Bhagavatula teaches a client system transmitting a request of authentication of the product to a server system at column 8, lines 20-25, which is reproduced as follows:

> On the other hand, if the user 40 passes the authentication procedure 302, the agent 10 administers a request processing procedure 308. The request processing procedure 308 retrieves the information or data requested by the user 40 from the respective vendors 30a-n, and forwards the same back to the user 40, e.g., via a requested information page 310.

(Bhagavatula, column 8, lines 19-25)

In this section, Bhagavatula describes that, in response to a user requesting access to personal and/or confidential information from one or more registered vendors and the user being authenticated by an agent, the agent retrieves the information or data requested by the user from the respective vendors and forwards the data back to the user. As presented in the Response to Office Action

filed February 11, 2008, Appellants respectfully submit the request sent by the user to the agent is for access to data from a vendor. Bhagavatula merely authenticates that the user "to ensure that the user 40 is registered and is in fact who he claims to be." (see Bhagavatula, column 7, lines 64-65) Nowhere in this section, or in any other section of Bhagavatula, is there a teaching of a client system transmitting a request of **authentication of the product** to a server system. That is, the request sent to Bhagavatula's agent is for access to vendor data. Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be.

In response to Appellant's argument, the Final Office Action alleges:

> The Examiner disagrees with argument. Bhagavatulat teaches requesting authentication of a product in col. 8, lines 20-25. Note the 'product' is interpreted equivalent to 'data requested by the user'. Applicant is also reminded although an attempt is made to cite the column and line numbers the entire reference must be considered. As for a 'server system' col. 8, line 27 teaches a server system.

(Final Office Action, pages 2-3, dated September 9, 2008)

In response to the Examiner's argument presented in the FOA, Appellants present here for the first time the following argument. Column 8, lines 20-25 of Bhagavatula describes that **the user is being authenticated** by an agent, not the data as alleged by the Examiner. In Bhagavatula, **the user** has to be

authenticated by the user prior to accessing the data. If the **user** is **authenticated**, then the agent retrieves the information or data requested by the user from the respective vendors and forwards the data back to the user. Additionally, while column 8, lines 27 may teach a server system, Bhagavatula still merely **authenticates** that **the user** "to ensure that the user 40 is registered and is in fact who he claims to be." (see Bhagavatula, column 7, lines 64-65) Nowhere in these sections, or in any other section of Bhagavatula, is there a teaching of a client system transmitting a request of **authentication** of **the product** to a server system.

Additionally, Bhagavatula fails to teach certifying that the product originates from the entity using sensitive information of the entity stored on the server system. The Final Office Action alleges that Bhagavatula teaches this feature at column 7, line 57 to column 8, line 25, which is reproduced as follows:

> By way of example, FIG. 4 shows user 40 accessing personal and/or confidential information from one or more registered vendors 30*a-n*. An authenticated data access process 300 begins with a registered user 40 contacting the agent 10, preferably, over the Internet 20. The agent 10 conducts an authentication procedure 302 to positively identify the user 40, i.e., to ensure that the user 40 is registered and is in fact who he claims to be. The authentication procedure 302 preferably includes the agent 10 presenting an authentication page to the use 40. The authentication page is set up to

collect authentication data from the user 40. Depending on the authentication vehicle set up for the user 40, the authentication data may include a user name or ID, a secret password, a dynamically changing password, a PIN, answers to security questions, biometric data, etc. The authentication data collected by the agent 10 is compared for consistency to the user account information maintained in the agent's database 14, and where there is a match, the user 40 is deemed authentic and positively identified as the holder of the matching account.

At decision step 304, it is determined if the user 40 has passed the authentication procedure 302. If the user 40 has not passed the authentication procedure 302, an access denied page 306 is returned to the user 40 informing him of his failure to be authenticated. Optionally, the access denied page 306 permits the user 40 to change and/or correct previously mis-entered authentication data and try again. The number of tries is, however, preferably limited.

On the other hand, if the user 40 passes the authentication procedure 302, the agent 10 administers a request processing procedure 308. The request processing procedure 308 retrieves the information or data requested by the user 40 from the respective vendors 30a n, and forwards the same back to the user 40, e.g., via a requested information page 310.

(Bhagavatula, column 7, line 57, to column 8, line 25)

As presented in the Response to Office Action filed February 11, 2008, Appellants respectfully submit this section Bhagavatula describes that, in response

to a user requesting access to personal and/or confidential information from one or more registered vendors and **the user** being **authenticated** by an agent, the agent retrieves the information or data requested by the user from the respective vendors and forwards the data back to the user. Again, the request sent by the user to the agent is for access to data from a vendor. Nowhere in this section, or in any other section of Bhagavatula, is there a teaching of **certifying** that **the product** originates from the entity using sensitive information of the entity stored on the server system. That is, the request sent to Bhagavatula's agent is for access to vendor data. Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be.

In response to Appellant's argument, the Final Office Action alleges:

> The Examiner disagrees with argument. Bhagavatula teaches the above limitation in col. 7, line 57 through col. 8, line 25. Note the sensitive information is equivalent to user name or ID, a secret password, a dynamically changing password, a PIN, answers to security questions, biometric data, etc .... which are taught in the Bhagavatula reference.

(Final Office Action, page 3, dated September 9, 2008)

In response to the Examiner's argument presented in the FOA, Appellants present here for the first time the following argument. Column 7, line 57, to column 8, line 25 describes that, in response to a user requesting access to

personal and/or confidential information from one or more registered vendors and **the user** being **authenticated** by an agent. The sensitive information used by Bhagavatula is for **authenticating the user** not the data as alleged by the Examiner. Thus as opposed to the allegation made by the Examiner, nowhere in this section, or in any other section of Bhagavatula, is there a teaching of **certifying** that **the product** originates from the entity using sensitive information of the entity stored on the server system.

Further, Bhagavatula fails to teach returning a representation of the certification to the client system. The Office Action alleges that Bhagavatula teaches this feature at column 7, line 57 to column 8, line 25, which is reproduced above. As presented in the Response to Office Action filed February 11, 2008, Appellants respectfully submit that Bhagavatula retrieves **the information or data requested by the user** from the respective vendors and forwards the data back to the user, in response to a user requesting access to personal and/or confidential information from one or more registered vendors and **the user** being **authenticated** by an agent. Nowhere in this section, or in any other section of Bhagavatula, is there a teaching of returning a representation of the **certification** that **the product originates from the entity** to the client system. Bhagavatula merely **authenticates the user** to ensure the user is registered and is in fact who he claims to be.

In response to Appellant's argument, the Final Office Action alleges:

> The Examiner disagrees with argument. Bhagavatula teaches the above limitation in col. 8, lines 54-67. Note the 'representation of the certification' is interpreted equivalent to the data selection page which is returned to the user.

(Final Office Action, page 3, dated September 9, 2008)

In response to the Examiner argument presented in the FOA, Appellants present here for the first time the following argument. As discussed above, the data accessed by the user is not authenticated. That is, Bhagavatula merely authenticates a user and if the user is authenticated the user is able to access the data. The **data** in Bhagavatula is **never authenticated**. That is, in Bhagavatula only **the user** is ever **authenticated**.

Therefore, Bhagavatula does not teach each and every feature of independent claim 1 as is required under 35 U.S.C. § 102(e). At least by virtue of their dependency on independent claim 1, the specific features of dependent claims 2 and 3 are not taught by Bhagavatula. Accordingly, Appellants respectfully request the rejection of claims 1-3 under 35 U.S.C. § 102(e) not be sustained.

Furthermore, Bhagavatula does not teach or provide a sound technical reason why the needed changes to reach the presently claimed invention are necessary. Absent the Office Action pointing out some teaching or incentive to

implement Bhagavatula such that a client system transmits a request of **authentication** of **the product** to a server system, the server system certifies that the product originates **from an entity** using sensitive information of the entity stored on the server system, and the server system returns a representation of the certification to the client system, as recited in independent claim 1, one of ordinary skill in the art would not be led to modify Bhagavatula to reach the present invention when the reference is examined as a whole. Absent some teaching or technical rational to modify Bhagavatula in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the Appellants' disclosure as a template to make the necessary changes to reach the claimed invention.

B.   Rejection under 35 U.S.C. § 103(a), Claims 4-8

The Final Office Action rejects claims 4-8 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Bhagavatula et al. (U.S. Patent No. 7,140,036) in view of Graves et al. (U.S. Publication No. 2004/0177047). This rejection is respectfully traversed.

The Final Office Action bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103.

In re Fritch, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). As presented

in the Response to Office Action filed February 11, 2008, Appellants respectfully

submit claims 4-7 are dependent on independent claim 1 and, thus, these claims

distinguish over Bhagavatula for at least the reasons noted above with regard to

claim 1. Moreover, Graves does not provide for the deficiencies of Bhagavatula

and, thus, any alleged combination of Bhagavatula and Graves would not be

sufficient to reject independent claim 1 or claims 4-7 by virtue of their

dependency. That is, Bhagavatula and Graves, taken alone or in combination, do

not teach or provide a technical reason for transmitting from a client system a

request of **authentication of the product** to a server system, certifying by a server

system that the product originates from the entity using sensitive information of

the entity stored on the server system, and returning by a server system a

representation of the certification to the client system.

In response to Appellant's argument, the Final Office Action alleges:

> The Examiner disagrees with argument. There are no
>
> deficiencies in Bhag.

(Final Office Action, page 3, dated September 9, 2008)

In response to the Examiner's argument presented in the FOA, Appellants

present here for the first time the following argument. Bhagavatula merely

authenticates the user to ensure the user is registered and is in fact who he claims

to be. Nowhere in this section, or in any other section of Bhagavatula, is there a teaching of a client system transmitting a request of **authentication of the product** to a server system. Thus, Appellants respectfully submit there is a deficiency in Bhagavatula in that Bhagavatula fails to teach or provide a technical reason for a client system to transmit a request of **authentication of the product** to a server system, certifying that **the product** originates from the entity using sensitive information of the entity stored on the server system, and returning a representation of the **certification** to the client system. Therefore, Bhagavatula is deficient. Furthermore, Bhagavatula and Graves, taken alone or in combination, fail to teach or provide a technical reason for the features of claims 4-7.

1.   **Claim 4**

As presented in the Response to Office Action filed February 11, 2008, Appellants respectfully submit Bhagavatula and Graves, taken alone or in combination, do not teach or provide a technical reason for where the step of certifying that the product originates **from an entity** using sensitive information of the entity stored on the server system includes automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key. The Office Action acknowledges that Bhagavatula does not teach these features, but alleges that Graves teaches where the step of certifying

that the **product originates from an entity** using sensitive information of the

entity stored on the server system includes automatically retrieving a private key

of the entity stored on the server system, and digitally signing the product using

the private key.

Graves is directed to an online commerce transaction system that

authenticates to a seller that a buyer is authorized to use a payment instrument as

part of an online commerce transaction with the seller. The authentication service

performs the following receives a request to verify that the buyer is authorized to

use the payment instrument. The authentication service determines whether the

buyer has access to certain secret information without revealing the secret

information to the seller. Access to the secret information verifies authority to use

the payment instrument. Responsive to the determination of whether the buyer has

access to the secret information, the authentication service transmits to the seller a

response including whether the buyer is authorized to use the payment instrument.

Thus, Graves merely describes authenticating whether a user is authorized

to use the payment instrument. The Final Office Action alleges that Graves

teaches where the step of certifying that the product originates **from an entity**

using sensitive information of the entity stored on the server system includes

automatically retrieving a private key of the entity stored on the server system, and

digitally signing the product using the private key in paragraphs [0050], [0052], and [0053], which are reproduced as follows:

> [0050]   The PTA and private keys may be hosted in a number of locations. In this example, a separate server (not shown) hosts the software implementing the PTA and stores the corresponding private keys. One advantage of this approach is that since the PTA and private keys are implemented as a zero-client, hosted service, no changes need be made to the buyer's browser. Another advantage is that since the buyer's browser does not require any special software, the buyer 110 potentially can access the PTA and his private keys from any standard browser. For an example of how this may be implemented, see co-pending U.S. patent application Ser. No. 09/574,687, "Server-Assisted Regeneration of a Strong Secret from a Weak Secret," by Warwick Ford, filed May 17, 2000, which subject matter is incorporated herein by reference. If the server hosting the PTA is the same as the one hosting the authentication service 130, the two functions may be integrated to some degree. In an alternate embodiment, the PTA and/or corresponding private keys are implemented on the buyer's client. For example, the PTA may be implemented as a plug-in (e.g., ActiveX control) to the buyer's browser and the private keys stored locally on the buyer's client or in dedicated hardware (e.g., a hardware token).

> [0052]   As a result of clicking the authenticated payment button 420, a request for authentication is sent 330 from the buyer's browser to

the authentication service 130. The request includes a description of the payment transaction and also identifies the seller 120. The authentication service 130 determines whether the buyer 110 has access to the secret information (in this case, the private key for the selected account) in steps 340-346. In particular, the authentication service 130 sends 340 a challenge request to the buyer 110. The challenge request asks the buyer 110 to digitally sign some data using the private key for the selected account. The buyer 110 sends 342 his challenge response back to the authentication service 130. The authentication service 130 retrieves the earlier stored public key and uses it to determine 346 whether the buyer 110 has access to the corresponding private key. The authentication process typically is carried out between computers without the human buyer 110's active participation.

[0053]   In this embodiment, the PTA is also invoked in order to allow the buyer 110 to select which of his accounts he wishes to use and later to select the specific payment instrument from within the account. More specifically, clicking button 420 causes the buyer's web browser to interact with the PTA via the dialog boxes in FIGS. 5A and 5B. In FIG. 5A, the buyer 110 specifies which account he wishes to use by filling in the User Name field 510 and then authenticates himself to the PTA by filling in the correct password 520. The PTA displays the dialog box of FIG. 5B, which includes a visual representation 530 of the account selected. The buyer 110 confirms that he wishes to use this account by clicking on the Login

button 540. The private key for the account is now available for authentication and digital signature.
(Graves, paragraphs [0050], [0052], and [0053])

In these paragraphs, Graves describes that, responsive to clicking an authenticated payment button, a request for authentication is sent from the buyer's browser to the authentication service. The request includes a description of the payment transaction and also identifies the seller. The authentication service determines whether the buyer has access to the secret information. The authentication service sends a challenge request to the buyer. The challenge request asks the buyer to digitally sign some data using the private key for the selected account. The buyer sends his challenge response back to the authentication service. The authentication service retrieves the earlier stored public key and uses it to determine whether the buyer has access to the corresponding private key.

As presented in the Response to Office Action filed February 11, 2008, Appellants respectfully submit that Graves authentication service does not automatically retrieve a private key of the entity, **from which the product originates**, that is stored on the server system in order to certify that the product originates **from an entity** using sensitive information of the entity stored on the server system. That is, Graves' authentication service receives a request from a

buyer **that authenticates whether a user is authorized to use the payment instrument.** The certificate does not certify **that the product** originates **from an entity** using sensitive information of the entity stored on the server system.

In response to Appellant's argument, the Final Office Action alleges:

> The Examiner disagrees with argument. Grave teaches the above limitation on pages 5-6, paragraphs 0050, 0052-0053 and 0058. Note in paragraph 0050, Graves teaches that the keys are stored on a separate server. Graves teaches that the PTA and authentication services can be integrated [0050] in addition the browser retrieves the appropriate key. As well as in paragraph 0059 that an automatically triggered client script can be used to eliminate the need to click through the intermediate pages. Applicant is also reminded although an attempt is made to cite the column and line numbers the entire reference must be considered.

(Final Office Action, page 4, dated September 9, 2008)

In response to the Examiner's argument presented in the FOA, Appellants present here for the first time the following argument. Appellants respectfully submit that simply integrating a Personal Trust Agent (PTA) and authentication and retrieving a key does not teach or provide a technical reason for automatically retrieving a private key of the entity, **from which the product originates**, that is stored on the server system, and digitally signing **the product** using the private key. Again, Graves merely **authenticates whether a user is authorized to use**

the payment instrument. The certificate does not certify **that the product** originates **from an entity** using sensitive information of the entity stored on the server system.

With regard to either paragraph [0058] or [0059], as the Examiner cites paragraph [0058] but refers to paragraph [0059], Appellants respectfully submit that neither paragraph [0058] nor [0059] teach or provide a technical rational for automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key. Appellants present here for the first time the following argument. In paragraph [0058], Graves describes that a form is served by the seller, but by the buyer clicking on the authenticated payment button hands off the buyer's browser from the seller to the authentication service. **Once the buyer is authenticated**, the buyer's browser is returned from the authentication service to the seller. In paragraph [0059], Graves describes that both of these transfers are accomplished using conventional techniques, such as GET, POST, and/or redirect. Appellants respectfully submit that merely handing off a service from a seller to an authentication service, merely handing off the service from the authentication service to the seller, or authenticating a buyer, does not teach or provide a technical reason for automatically retrieving a private key of the entity, **from which the product originates**, stored on the server system, and digitally signing the product using the private key.

Thus, in addition to being dependent on independent claim 1, the specific features of dependent claim 4 is also distinguishable over Bhagavatula and Graves, taken alone or in combination, by virtue of the specific feature recited in these claims. Accordingly, Appellants respectfully request the rejection of dependent claim 4 under 35 U.S.C. § 103(a) not be sustained.

2. Claim 7

As presented in the Response to Office Action filed February 11, 2008, Appellants respectfully submit Bhagavatula and Graves, taken alone or in combination, do not teach or provide a technical reason for the client system invoking a remote command on the server system, the server system verifying whether the remote command is included in a predefined list stored on the server system, the list including at least one remote command for satisfying the request of authentication, and the server system executing the remote command if included in the list. The Office Action alleges that Graves teaches this feature in paragraphs [0050], [0052], and [0053], which are reproduced above. As described above, Graves merely authenticates whether a user is authorized to use the payment instrument. Appellants respectfully submit that Graves' authentication service does not verify whether the remote command is included in a predefined list stored on the server system. At most, Graves merely sends a challenge request to the

buyer, asks the buyer to digitally sign some data using the private key for the selected account, sends this challenge response back to the authentication service, and retrieves the earlier stored public key and uses it to determine whether the buyer has access to the corresponding private key. Nowhere in the Graves reference is there a teaching or technical reason that the certificate from the user is compared to a list of certificates, much less a list that includes at least one remote command for satisfying the request of authentication.

In response to Appellant's argument, the Final Office Action alleges:

> The Examiner disagrees with argument. Grave teaches the above limitation on page 6, paragraph 0053. Note the remote command is interpreted equivalent to private key and digital signature now available by selecting the account.

(Final Office Action, page 4, dated September 9, 2008)

In response to the Examiner's argument presented in the FOA, Appellants present here for the first time the following argument. Graves is directed to **authenticating whether a user is authorized to use a payment instrument**. In paragraph [0053], the Personal Trust Agent (PTA) is also invoked in order to allow the buyer to select which of his accounts he wishes to use and later to select the specific payment instrument from within the account. By clicking the button causes the buyer's web browser to interact with the PTA via dialog boxes. The buyer specifies which account he wishes to use by filling in the User Name field

and **then authenticates himself** to the PTA by filling in a correct password. The PTA displays a dialog box, which includes a visual representation of the account selected. The buyer confirms that he wishes to use this account by clicking on the Login button. The private key for the account is now available for authentication and digital signature. Thus, Graves merely **authenticates whether a user is authorized to use the payment instrument**. Appellants respectfully submit that Grave's private key, **of the buyer** , that is used for authentication and digital signature, **of the buyer**, is not equivalent to the client system invoking a remote command on the server system, the server system verifying whether the remote command is included in a predefined list stored on the server system, the list including at least one remote command for satisfying the request of authentication, **of the product**, and the server system executing the remote command if included in the list.

Thus, in addition to being dependent on independent claim 1, the specific features of dependent claim 7 is also distinguishable over Bhagavatula and Graves, taken alone or in combination, by virtue of the specific feature recited in these claims. Accordingly, Appellants respectfully request the rejection of dependent claim 7 under 35 U.S.C. § 103(a) not be sustained.

3. Claim 8

As presented in the Response to Office Action filed February 11, 2008, Appellants respectfully submit that similar distinctions of the claims over the Bhagavatula as discussed above with respect to claim 1, apply to independent claim 8. Claim 8 recites "**a client system transmitting a request of authentication of the product to a server system**, the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification: **generating a digital signature of the product using a private key of the entity stored on the server system**, and **returning the digital signature to the client system, wherein the digital signature certifies that the product originates from the entity**." (emphasis added). Graves does not provide for the deficiencies of Bhagavatula and, thus, any alleged combination of Bhagavatula and Graves would not be sufficient to reject independent claim 8. That is, Bhagavatula and Graves, taken alone or in combination, do not teach or provide a technical reason for transmitting from a client system a request of authentication of the product to a server system, certifying by a server system that the product originates from the entity using sensitive information of the entity stored on the server system, and returning by a server system a representation of the certification to the client system.

The Office Action alleges that Graves teaches generating a digital signature of the product using a private key of the entity stored on the server system in paragraphs [0050], [0052], and [0053], which are reproduced above. Again, in these sections, Graves merely authenticates whether a user is authorized to use the payment instrument. Appellants respectfully submit that one of ordinary skill in the art would not confuse Grave's generation of authentication challenge for a buyer to that authenticates whether a user is authorized to use the payment instrument with the presently claimed generating a digital signature of the product that certifies that the product originates **from an entity** using sensitive information of the entity stored on the server system.

Additionally, the Office Action alleges that Graves teaches returning the digital signature to the client system, wherein the digital signature certifies that the product originates from the entity in paragraph [0056], which is reproduced as follows:

> [0056]   The buyer 110 and authentication service 130 create 380 a digitally signed record of the transaction using the form and dialog box shown in FIGS. 7A and 7B. In response to the submission of the form 600, the authentication service 130 returns the form of FIG. 7A which contains a summary 710 of the transaction and requests that the buyer 110 authorize the transaction. The buyer 110 does so by clicking on the Authorize Transaction button 720. This invokes the

PTA dialog box of FIG. 7B. By clicking the Sign button 730, the

buyer causes the PTA to digitally sign the summary, thus creating a

digitally signed record of the transaction. The authentication service

130 then notifies 350 the seller 120 that the buyer is authorized to use

the payment instrument and preferably also notifies the buyer that the

transaction was approved.

(Graves, paragraphs [0056])

In this paragraph, Graves describes creating a digitally signed record of a

transaction and the authentication service returning a form which contains a

summary of the transaction and requests that the buyer authorize the transaction.

Appellants respectfully submit one of ordinary skill in the art would not confuse

returning a record of transaction with returning the digital signature to the client

system, wherein the digital signature certifies that the product originates from the

entity.

Furthermore, no technical rational is present in any of the references to

modify the references to include such a feature. That is, there is no teaching or

technical rational in Bhagavatula and Graves, taken alone or in combination, that a

problem exists for which transmitting from a client system a request of

authentication of the product to a server system, certifying by a server system that

the product originates from the entity using sensitive information of the entity

stored on the server system, and returning by a server system a representation of

the certification to the client system, is a solution. To the contrary, Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be. Graves merely describes authenticating whether a user is authorized to use the payment instrument. Neither of the references certifies at a server system that **a product** originates **from an entity** using sensitive information of the entity stored on the server system.

Moreover, neither reference teaches or provides a technical rational for incorporating the subject matter of the other reference. That is, there is no motivation offered in either reference for the alleged combination. The Office Action alleges that the motivation would be "because there is a need for buyer authentication in online purchases." The present invention provides for a server system that **certifies** that **the product** originates from the entity using sensitive information of the entity stored on the server system. As discussed above, Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be and Graves merely describes authenticating whether a user is authorized to use the payment instrument. Neither reference teaches or provides a technical reason for the presently claimed features. Thus, the only teaching or technical rational to even attempt the alleged combination is based on a prior knowledge of Appellants' claimed invention thereby constituting

impermissible hindsight reconstruction using Appellants' own disclosure as a guide.

One of ordinary skill in the art, being presented only with Bhagavatula and Graves, and without having a prior knowledge of Appellants' claimed invention, would not have found it obvious to combine and modify Bhagavatula and Graves to arrive at Appellants' claimed invention, as recited in claims 1 or 8. To the contrary, even if one were somehow motivated to combine Bhagavatula and Graves, and it were somehow possible to combine the systems, the result would not be the invention as recited in claims 1 or 8. The resulting system would be verifying that a user has access to download the executable file prior to downloading the file. The resulting system would still fail to transmit a request of authentication of the product to a server system, certify at a server system that the product originates from the entity using sensitive information of the entity stored on the server system, and return from a server system a representation of the certification to the client system.

In response to Appellant's argument, the Final Office Action alleges:

> The Examiner disagrees with argument for multiple reasons. First, Bhagavatula teaches the limitations as argued with respect to claim 1 as shown above. Second, as shown in the Office Action Graves teach the limitation of generating a digital signature as stated in paragraph 0050, 0052, and 0053. As known and repeated by

Applicant Grave's invention is utilized to authenticate a user for a payment instrument. This teaching does not take away the teachings of Graves automatically generating a digital signature by selection of account also see paragraph 0059.

(Final Office Action, pages 4-5, dated September 9, 2008)

In response to the Examiner's argument presented in the Final Office Action, Appellants present here for the first time the following argument. The Examiner acknowledges that Graves is utilized to **authenticate a user** for a payment instrument. Appellants respectfully submit that Bhagavatula merely **authenticates the user** to ensure the user is registered and is in fact who he claims to be. Neither reference teaches or provides a technical reason for a client system transmitting a request of **authentication of the product** to a server system, the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification: generating **a digital signature of the product** using a private key of the entity stored on the server system, and returning the digital signature to the client system, wherein the digital signature **certifies that the product originates from the entity**.
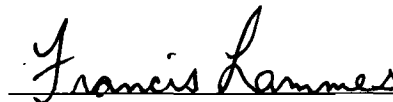
In view of the above, Appellants respectfully submit that Bhagavatula and Graves, taken alone or in combination, fail to teach or provide a technical rational for the features of claim 8. Accordingly, Appellants respectfully request the rejection of independent claim 8 under 35 U.S.C. § 103(a) not be sustained.

C. <u>Conclusion</u>

In view of the above, Appellants respectfully submit that claims 1-8 of the present application are directed to statutory subject matter and that the features of these claims are not taught or technically reasoned by the 1-8 references. Accordingly, Appellants request that the Board of Patent Appeals and Interferences overturn the rejections set forth in the Final Office Action.

Respectfully submitted,

Francis Lammes
Reg. No. 55,353
Walder Intellectual Property Law, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
Phone: (972) 380-9475
Fax: (972) 733-1575
Email: lammes@walderiplaw.com
AGENT FOR APPELLANTS

X.   Appendix

A.   Claims

1.   (Rejected) A method of authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the method including the steps of:

a client system transmitting a request of authentication of the product to a server system,

the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:

certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and

returning a representation of the certification to the client system.

2.   (Rejected) The method according to claim 1, wherein the step of verifying whether the request is received from an authorized subject includes:

comparing an address of the client system with an indication of authorized addresses stored on the server system.

3.   (Rejected) The method according to claim 1, wherein the step of verifying

whether the request is received from an authorized subject includes:

comparing an identifier of a user logged on the client system with an

indication of authorized users stored on the server system.

4.   (Rejected) The method according to claim 1, wherein the step of certifying

includes:

automatically retrieving a private key of the entity stored on the server

system, and

digitally signing the product using the private key.

5.   (Rejected) The method according to claim 4, wherein the step of

automatically retrieving the private key includes:

calling a signing command passing a password for accessing the private key

as a parameter.

6.   (Rejected) The method according to claim 4, wherein the step of

automatically retrieving the private key includes:

calling a signing command with an option causing the import of the private

key from a private configuration memory area of the server system.

7.   (Rejected) The method according to claim 1, further including the steps of:

the client system invoking a remote command on the server system, the

server system verifying whether the remote command is included in a predefined

list stored on the server system, the list including at least one remote command for

satisfying the request of authentication, and

the server system executing the remote command if included in the list.

8.   (Rejected) A method of authenticating a software product being originated

by an entity having at least one authorized subject, the method including the steps

of:

a client system transmitting a request of authentication of the product to a

server system,

the server system verifying whether the request is received from an

authorized subject, and responsive to a positive verification:

generating a digital signature of the product using a private key of the

entity stored on the server system, and

returning the digital signature to the client system, wherein the digital

signature certifies that the product originates from the entity.

9-19. (Canceled)

B. Claims Support and Drawing Analysis

1. A method of authenticating a digitally encoded product being originated by

an entity having at least one authorized subject {**e.g. page 15, lines 16-19**}, the

method including the steps of:

a client system {**e.g. page 10, line 35, and 'client' of Figure 3a**}

transmitting {**e.g. page 11, lines 7-9, and element 315 of Figure 3a**} a request of

authentication {**e.g. page 11, line 8**} of the product {**e.g. page 8, lines 31-33, and**

page 11, lines 4-9} to a server system{**e.g. page 11, line 9**},

the server system{**e.g. page 11, line 9**} verifying {**e.g. page 11, lines 20-24,**

and element 335 of Figure 3a} whether the request {**e.g. page 11, line 8**} is

received from an authorized subject{**e.g. page 11, lines 20-24**}, and responsive to

a positive verification{**e.g. page 11, lines 28-31, and element 349 of Figure 3a**}:

certifying {**e.g. page 12, lines 3-12**} that the product {**e.g. page 12,**

lines 8-9, and element 510 of Figure 5} originates from the entity {**e.g.**

page 12, lines 3-5 and 18-20, and SCRa of Figure 3b} using sensitive

information {**e.g. page 12, lines 12-18**} of the entity {**e.g. page 12, lines 3-5**

and 8-20} stored on the server system{**e.g. page 11, line 9**}, and

returning {e.g. page 12, lines 24-26, and element 363 of Figure 3b}

a representation of the certification {e.g. page 12, lines 24-26} to the client

system{e.g. page 12, lines 21-26}.

4.   The method according to claim 1, wherein the step of certifying includes:

automatically retrieving {e.g. page 13, lines 7-10, and element 372 of

Figure 3b} a private key {e.g. page 13, line 10} of the entity {e.g. page 13, line 4}

stored on the server system{e.g. page 11, line 9}, and

digitally signing {e.g. page 13, lines 17-18, and element 375 of Figure 3b}

the product {e.g. page 8, lines 31-33, page 11, lines 4-9} using the private

key{e.g. page 13, line 10}.

7.   The method according to claim 1, further including the steps of:

the client system {e.g. page 10, line 35} invoking {e.g. page 11, lines 17-19,

and element 330 of Figure 3a} a remote command {e.g. page 11, line 15} on the

server system{e.g. page 11, line 9}, the server system {e.g. page 11, line 9}

verifying {e.g. page 11, lines 25-27} whether the remote command {e.g. page 11,

line 26} is included in a predefined list {e.g. page 11, line 27} stored on the server

system{e.g. page 11, line 9}, the list {e.g. page 11, line 27} including at least one

remote command {**e.g. page 11, line 26**} for satisfying the request of

authentication, and

the server system {**e.g. page 11, line 9**} executing {**e.g. page 11, lines 28-**

31, and element 349 of Figure 3a} the remote command {**e.g. page 11, line 30**} if

included in the list{**e.g. page 11, line 27**}.

8.   A method of authenticating a software product being originated by an entity

having at least one authorized subject {**e.g. page 15, lines 16-19**}, the method

including the steps of:

a client system {**e.g. page 10, lines 35, and 'client' of Figure 3a**}

transmitting {**e.g. page 11, lines 7-9, and element 315 of Figure 3a**} a request of

authentication {**e.g. page 11, line 8**} of the product { **e.g. page 8, lines 31-33, and**

page 11, lines 4-9} to a server system{**e.g. page 11, line 9**},

the server system {**e.g. page 11, lines 9**} verifying {**e.g. page 11, lines 20-**

24, and element 335 of Figure 3a} whether the request {**e.g. page 11, line 8**} is

received from an authorized subject{**e.g. page 11, lines 20-24**, and responsive to a

positive verification{**e.g. page 11, lines 28-31, and element 349 of Figure 3a**}:

generating {**e.g. page 13, lines 17-18, and element 375 of Figure**

3b} a digital signature {**e.g. page 13, lines 17-18**} of the product {**e.g. page**

12, lines 8-9} using a private key {e.g. page 13, line 10} of the entity {e.g.

page 13, line 4} stored on the server system{e.g. page 11, line 9}, and

returning {e.g. page 13, lines 19-22, and element 378 of Figure 3b}

the digital signature {e.g. page 13, line 19} to the client system{e.g. page

13, lines 21-22}, wherein the digital signature {e.g. page 13, line 19}

certifies that the product {e.g. page 12, lines 8-9} originates from the

entity{e.g. page 13, line 4}.

C.   **Means or Step Plus Function Analysis**

        NONE

D.   **Evidence**

        NONE

E.   **Related Cases**

        NONE